Christyne M. Martens WSB #7-5044
Assistant United States Attorney
District of Wyoming
P.O. Box 22211
Casper, WY 82602
307-261-5434 (phone)
307-261-5471 (fax)
christyne.martens@usdoj.gov

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF WYOMING

UNITED STATES OF AMERICA, **Plaintiff,** **v.** **CODY DONOVAN SMITH,** **Defendant.**	**Criminal No. 20-CR-45-F**

GOVERNMENT'S COMBINED MOTION IN LIMINE TO AUTHENTICATE RECORDS AND NOTICE OF INTENT TO PROCEED UNDER FED. R. EVID 902(11), 902(13), AND 803(6)

The United States of America, by and through its attorney, Christyne M. Martens, Assistant United States Attorney for the District of Wyoming, hereby files its motion in limine to authenticate Apple, Verizon, Sprint, and Tinder records pursuant to Federal Rules of Evidence 902(11) and 902(13) and the data acquisition file from Smith's iPhone 8 pursuant to Federal Rules of Evidence 902(11) and 902(14). This motion in limine shall also serve as a formal notice of the government's intent to introduce the records referenced below pursuant to Federal Rules of Evidence 902(11), 902(13), and 902(14).

Pursuant to General Order 2020-11, which serves as an addendum to U.S.D.C.L.Cr.R. 47.1(a), the undersigned counsel has repeatedly attempted to confer with counsel for Smith without success.

I. Introduction and Factual Background

On March 18, 2020, the grand jury indicted Smith on one count of kidnapping in violation of 18 U.S.C. § 1201(a)(1) and one count of abusive sexual contact in violation of 18 U.S.C. § 2244(a)(1). (Doc. 1). Trial is scheduled to commence May 10, 2021. (Doc. 59). During the investigation, Special Agent Jake Olson served search warrants on Apple, Verizon, Sprint, and Tinder. Pursuant to the warrants, each company produced records and provided business records certifications, which are attached here as Exhibits 1-4. A search warrant also authorized the search of Smith's iPhone 8, seized from him at the time of his arrest, and Federal Bureau of Investigation IT Specialist-Forensic Examiner James Stevens acquired the data from that device. His certification is attached here as exhibit 5.

The United States brings this motion to simplify and shorten the jury trial in this matter by making the testimony of at least five witnesses unnecessary. Federal Rules of Evidence 902(11) provides that "certified records of regularly conducted activity" are self-authenticating. Beginning in December of 2017, rule 902(13) and 902(14) also provide that "certified records generated by an electronic process or system" and "certified data copied from an electronic device, storage medium, or file" are self-authenticating. Based on these rules, the United States seeks to pre-authenticate the Apple, Verizon, Sprint, and Tinder records along with the data acquisition file from Smith's iPhone 8. (Exhibit 1-5).

In order to authenticate these records, the United States intends to send each witness a subpoena for their trial testimony unless either: the Court grants this motion and finds their

authentication testimony unnecessary; or defendant stipulates to the authenticity of the underlying records. Thus, the United States has brought this motion in an effort to avoid wasting the time and resources of this Court, the jury, and at least five witnesses — whom would likely be required to travel to testify, despite the ongoing Covid-19 pandemic.

To be clear, even if the Court grants this motion, the records at issue will still be subject to other challenges. *See* Fed. R. Evid. 902(13), advisory committee's note to 2017 amendment ("A certification under this Rule can establish only that the proffered item has satisfied the admissibility requirements for authenticity. The opponent remains free to object to admissibility of the proffered item on other grounds. . . ."). Thus, this motion serves to simply authenticate the records – an uncontroversial premise – in advance of trial to conserve the resources of the Court, the jury, the parties, and the witnesses.

II. The Apple, Verizon, Sprint, and Tinder records are self-authenticating

"The court must decide any preliminary question about whether . . . evidence is admissible. In so deciding, the court is not bound by evidence rules, except those on privilege." Fed. R. Evid. 104(a). A determination as to whether evidence may be self-authenticated under Rule 902 and 803(6) is such a preliminary determination.

"To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is." Fed. R. Evid. 901(a). However, certain types of evidence are "self-authenticating" and therefore "require no extrinsic evidence of authenticity in order to be admitted." Fed. R. Evid. 902; *United States v. Arnold*, 696 Fed.Appx. 903, 906 (10th Cir. 2017) ("[W]hen evidence is self-authenticating under rule 902, it necessarily satisfies Rule 901(a).")

Certified domestic records of a regularly conducted activity are self-authenticating where:

> The original or a copy of a domestic record that meets the requirements of Rule 803(6)(A)-(C), as shown by a certification of the custodian or another qualified person that complies with a federal statute or a rule prescribed by the Supreme Court. Before the trial or hearing, the proponent must give an adverse party reasonable written notice of the intent to offer the record--and must make the record and certification available for inspection--so that the party has a fair opportunity to challenge them.

Fed. R. Evid. 902(11).

Here, the Apple, Verizon, Sprint, and Tinder records have been made available to Smith, the custodians' certificates of authenticity have been supplied him in discovery, and he has received notice of the government's intention to rely on the certificates through first seeking his stipulation by email on December 11, 2020, and this pleading. Meeting the final requirement of Rule 902(11), the certificates show that the Apple, Verizon, Sprint, and Tinder records are business records satisfying Rule 803(6)(A)-(C).

Rule 803(6) provides that records of regularly conducted activities are excluded from the rule against hearsay if:

> (A) the record was made at or near the time by--or from information transmitted by--someone with knowledge;
>
> (B) the record was kept in the course of a regularly conducted activity of a business, organization, occupation, or calling, whether or not for profit;
>
> (C) making the record was a regular practice of that activity;
>
> (D) all these conditions are shown by the testimony of the custodian or another qualified witness, or by a certification that complies with Rule 902(11) or (12) or with a statute permitting certification; and
>
> (E) the opponent does not show that the source of information or the method or circumstances of preparation indicate a lack of trustworthiness.

Fed. R. Evid. 803(6).

Each of the certificates provides that the custodian of records works at the company that produced the records and is authorized to certify the records, the custodian reviewed the records

produced, the records are an exact copy kept as part of Apple's, Verizon's, Sprint's, or Tinder's records regularly conducted activity, and that the records were made at or near the time the information was transmitted by the user. Thus, the Apple, Verizon, Sprint, and Tinder records are business records that satisfy the requirements of Rule 803(6)(A)-(C), which in turn satisfies 902(11).

These records are similarly self-authenticating as certified records generated by an electronic process or system: "A record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent must also meet the notice requirements of Rule 902(11)." Fed. R. Evid. 902(13). As explained above, the certificates show that these records are self-authenticating under Rule 902(11). The certificates also show that the records are an exact copy of the records generated by Apple's, Verizon's, Sprint's, and Tinder's automated systems. Thus, Rule 902(13) is also satisfied.

III. The data acquisition file of Smith's iPhone 8 is self-authenticating.

Finally, the government seeks to authenticate the data acquisition file of Smith's iPhone 8, seized from him at the time of his arrest. That authentication is accomplished by the declaration of and Federal Bureau of Investigation IT Specialist-Forensic Examiner James Stevens, which is Exhibit 5.

Under Rule 902(14), "[d]ata copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person" is self-authenticating evidence. Fed. R. Evid. 902(14). As with evidence under Rule 902(13), "A proponent establishing authenticity under this Rule must present a certification

containing information that would be sufficient to establish authenticity were that information provided by a witness at trial." *Id*., Advisory Committee's Note (2017).

The certification provided in Exhibit 5 establishes that the certifier, IT Specialist-Forensic Examiner Stevens (1) made a complete and accurate image of the iPhone 8; (2) was qualified to do so; and (3) confirmed that the hash of the original drive matched the hash of the imaged copy, as contemplated by the Rules Committee.[1]

Note that the sole purpose of IT Specialist-Forensic Examiner Stevens' certification is to authenticate the data acquisition file of Smith's iPhone. The fact that the phone belonged to defendant will be established at trial, not simply by the fact that it was obtained from defendant's person at the time of his arrest, but also based on the contents of the device. *See* Fed. R. Evid. 901(b)(4) (noting that evidence may be authenticated based on "[t]he appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances"). The witness who examined the phone and reviewed its contents will testify at trial and will be subject to cross-examination.

IV. The Confrontation Clause does not prevent the admission of self-authenticating records.

The Confrontation Clause of the Sixth Amendment does not prevent these records from being self-authenticated. The Confrontation Clause "guarantees a defendant's right to confront those 'who bear testimony' against him." *Melendez-Diaz v. Massachusetts*, 557 U.S. 305, 309 (2009) (quoting *Crawford v. Washington*, 541 U.S. 36, 51 (2004)). Thus, for an out-of-court

[1] *See* Fed. R. Evid. 902(14), Advisory Committee's Note (2017) ("Today, data copied from electronic devices, storage media, and electronic files are ordinarily authenticated by 'hash value'. A hash value is a number that is often represented as a sequence of characters and is produced by an algorithm based upon the digital contents of a drive, medium, or file. If the hash values for the original and copy are different, then the copy is not identical to the original. If the hash values for the original and copy are the same, it is highly improbable that the original and copy are not identical. Thus, identical hash values for the original and copy reliably attest to the fact that they are exact duplicates. This amendment allows self-authentication by a certification of a qualified person that she checked the hash value of the proffered item and that it was identical to the original.")

testimonial statement to be admissible against a defendant at trial, the declarant must testify or, if the declarant is now unavailable, the defendant must have had a previous opportunity to cross-examine the declarant. *United States v. Yeley-Davis*, 632 F.3ed 673, 678 (10th Cir. 2011) (citing *United States v. Pablo*, 625 F.3d 1285 (10th Cir. 2010)).

The Tenth Circuit examined these protections and held that cell phone records are business records and that the accompanying certificate of authenticity offered under Rule 902(11) was not testimonial. *Yeley-Davis*, 632 F.3d at 678-81. In reaching this conclusion, the court relied on the suggestion in *Crawford* that "business records are, by nature, not testimonial, and therefore not subject to the Confrontation Clause" that was later reaffirmed by the Supreme Court in *Melendez-Diaz*. *Id*. at 679. In rejecting the contention to the contrary, the Tenth Circuit explained that the certification authenticating the cell phone records asserted that the information had been kept in Verizon's regular course of business, which defeated the notion that the records had been prepared solely for litigation. *Id*.

By rejecting the contention that certificates under Rule 902 were testimonial, the Tenth Circuit joined other circuit courts of appeal to reach the same conclusion. *Id*. at 680-81; *see also United States v. Weiland*, 420 F.3d 1062, 1077 (9th Cir. 2005) ("[A] routine certification by the custodian of a domestic public record . . . and a routine attestation to authority and signature . . . are not testimonial in nature."). Consequently, there is no constitutional barrier to the self-authentication of these records.

IV. Smith should affirmatively challenge the self-authentication of the Apple, Verizon, Sprint, and Tinder records and the data acquisition of his iPhone 8 or this Court should deem any objection waived.

While Smith has not agreed to stipulate to the self-authenticating nature of the records, his refusal to do so should not require the government to summon a witness to testify in-person at trial

without more. A district court does not abuse its discretion by allowing the government to rely on certificates of authenticity at trial, without live witness testimony, despite a defendant's objection. *United States v. Jenkins*, 540 Fed. Appx. 893, 897, 899-901 (10th Cir. 2014) (affirming on appeal the use of certificates of authenticity despite defendant's trial objection).

While the government could bet on this Court's favorable ruling at trial by relying on the certificates and failing to produce a live witness, the Federal Rules of Evidence do not require such a gambit. Rule 902(11) allows the opponent of the evidence a fair opportunity to challenge the authenticity of the evidence after reasonable notice. Fed. R. Evid. 902(11). And an opponent of business records under the hearsay rule must show a lack of trustworthiness to prevent their admission. Fed. R. Evid. 803(6)(E). Therefore, both rules contemplate some sort of affirmative challenge to the admission of such evidence.

This reading is consistent with the purpose of the rules. In enacting Rule 902(13) and (14), the Advisory Committee explained that "as with the provisions on business records in Rules 902(11) and (12), the Committee has found that the expense and inconvenience of producing a witness to authenticate an item of electronic evidence is often unnecessary." Fed. R. Evid. 902, advisory committee's note to 2017 amendment. "It is often the case that a party goes to the expense of producing an authentication witness, and then the adversary either stipulates authenticity before the witness is called or fails to challenge the authentication testimony once it is presented." *Id*.

Neither the rule, nor an order from this Court provides any deadline for Smith to challenge the government's use of Rules 902(11), 902(13), and 902(14). And while Smith has not agreed to stipulate to the government's reliance on the certificates of authenticity, there is no guarantee he will actually offer any challenge to the evidence at trial. Therefore, to effectuate the purpose of the rule—to avoid unnecessary cost and inconvenience to the Court, parties, jurors, and witnesses—

Smith should make any challenge he has in response to this motion or this Court should deem it waived. This will allow the Court to make a pretrial determination should he make a meaningful challenge and allow the government and its witnesses to plan accordingly.

III. CONCLUSION

The government only seeks to alleviate the need for the custodians of Apple's, Verizon's, Sprint's, and Tinder's records and IT Specialist-Forensic Examiner Stevens to appear and testify to the contents of their affidavits at trial. The ruling would not limit Smith's ability to challenge the evidence on other grounds. Thus, the government respectfully requests that the Court conclude that the certificates attached as Exhibit 1-4 show that the Apple, Verizon, Sprint, and Tinder records are business records that satisfy Rules 902(11), and 902(13) and that live witness testimony is unnecessary to authenticate the related records. The government further requests that this Court finds that IT Specialist-Forensic Examiner Stevens' declaration, Exhibit 5, satisfies Rule 902(14) and that his testimony is not necessary at trial to authenticate the data acquisition file of Smith's iPhone 8.

DATED this 9th day of April, 2020.

Respectfully submitted,

L. ROBERT MURRAY
Acting United States Attorney

By: */s/ Christyne M. Martens*
CHRISTYNE M. MARTENS
Assistant United States Attorney

CERTIFICATE OF SERVICE

I hereby certify that on April 9, 2021, the foregoing was electronically filed and consequently served on defense counsel via the CM/ECF, the Court's Electronic Filing System.

/s/ Andi M. Shaffer
UNITED STATES ATTORNEY'S OFFICE